2017/09/16, 2017 보안 기초 세미나

TCP/IP 완벽 가이드

- II-5부 IP 관련 기능 프로토콜 -

최창준 (changjun@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

- 보 충
  - IP 라우팅과 멀티캐스팅
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

IP 라우팅과 멀티캐스팅

- IP 패킷 전달
  - 직접 패킷 전달
    - 동일한 네트워크의 두 장비간에 패킷이 송수신될 때는 출발지 장비에서 목적지 장비로 직접 패킷 전달
  - 간접 패킷 전달(라우팅)
    - 동일한 네트워크에 있지 않을 경우의 패킷 전달
    - 출발지 장비는 외부 네트워크의 목적지 장비를 볼 수 없기 때문에 하나 이상의 중간 장비를 통해 전달

IP 라우팅과 멀티캐스팅

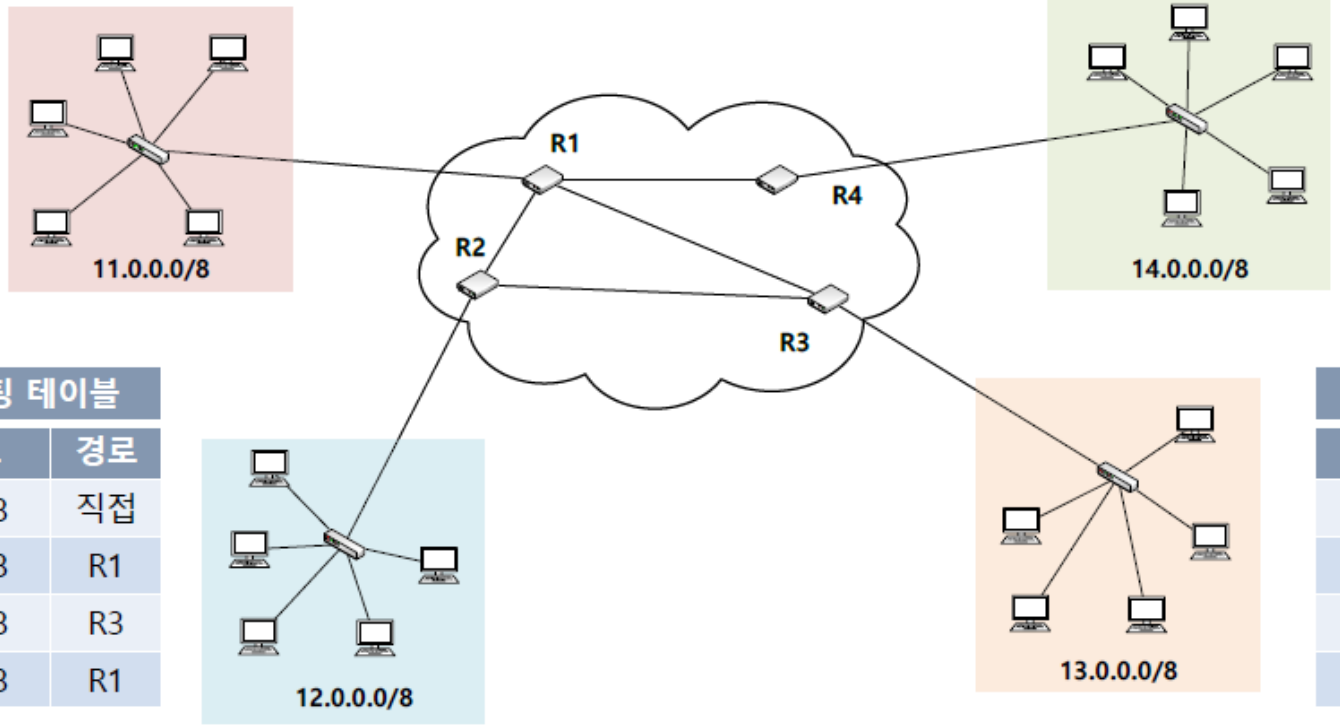
- IP 패킷 전달
  - 패킷 라우팅과 주소 지정의 관계
    - 클래스 단위 주소 지정
      - 클래스를 파악하고 네트워크 ID를 확인하여 라우팅 결정
    - 서브넷 클래스 단위 주소 지정
      - 서브넷 마스크를 통해 네트워크 ID, 서브넷 ID를 확인하여 라우팅 결정
    - 클래스 비사용 주소 지정
      - 서브넷 ID가 존재하지 않음
      - 슬래시 숫자를 이용하여 네트워크 ID 확인 후 라우팅 결정

IP 라우팅과 멀티캐스팅

- IP 라우팅과 홉
  - 라우팅(Routing)
    - 목적지로 가는 경로를 설정해주는 과정
    - 한 번에 한 홉씩 수행
  - 다음 홉 라우팅(Next-Hop Routing)
    - 한 라우터에서 다음 라우터로의 전달 과정
  - 홉 수(Hop Count)
    - 라우터의 수

IP 라우팅과 멀티캐스팅

- IP 경로와 라우팅 테이블
  - IP 주소가 로컬 장비가 아닐 경우 다음 라우터를 결정하는데 어떤 장비로 보내야 할지를 결정해야 함
    - 자신과 연결된 라우팅들과 라우팅 매핑 정보 모음을 관리



R1 라우팅 테이블

네트워크	경로
11.0.0.0/8	직접
12.0.0.0/8	R2
13.0.0.0/8	R3
14.0.0.0/8	R4

R2 라우팅 테이블

네트워크	경로
12.0.0.0/8	직접
11.0.0.0/8	R1
13.0.0.0/8	R3
14.0.0.0/8	R1

R3 라우팅 테이블

네트워크	경로
13.0.0.0/8	직접
11.0.0.0/8	R1
12.0.0.0/8	R2
14.0.0.0/8	R1

R4 라우팅 테이블

네트워크	경로
14.0.0.0/8	직접
11.0.0.0/8	R1
12.0.0.0/8	R1
13.0.0.0/8	R1

IP 라우팅과 멀티캐스팅

- IP 멀티캐스팅
  - 한 장비가 여러 특정 그룹의 수신자 장비에게 패킷을 전송하는 것
  - 주요 기능
    - 멀티캐스트 주소 지정
      - 자신에게 수신될 패킷을 기다리는 장비의 멀티캐스트 그룹을 식별
    - 멀티캐스트 그룹 관리
      - 동적으로 그룹에 참여, 탈퇴할 수 있음
      - 그룹 정보는 IP 인터네트워크로 전파
        - IGMP(Internet Group Management Protocol) 사용
          - 인터넷의 장비와 라우터들이 서로 그룹과 그 그룹 가입 정보를 교환할 수 있도록 하는 메시지 포맷

IP 라우팅과 멀티캐스팅

- IP 멀티캐스팅
  - 주요 기능
    - 멀티캐스트 패킷 처리와 라우팅
      - 하나의 장비에서 여러 장비로 송신하기 때문에 패킷의 사본 필요
        - 라우터는 언제 사본을 만들어야 하는지 파악
    - 패킷을 포워딩할 특수 알고리즘 사용
      - 사본을 생성하기 때문에 불필요한 트래픽 처리를 감소 시켜야 함
      - 거리 벡터 멀티캐스트 라우팅 프로토콜(DVMRP, Distance Vector Multicast Routing Protocol)
      - 최단 경로 우선 알고리즘(SPFA, Shortest Path First Algorithm)
    - 라우터는 최초 송신 장비가 그룹의 구성원이 아니더라도 멀티캐스트 그룹으로 송신된 패킷을 처리할 수 있어야 함

목 차

- 보 충
  - IP 라우팅과 멀티캐스팅
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT, Network Address Translation)
  - IP 패킷을 라우팅하여 기관의 사설 네트워크에서 온 패킷을 공인 IP 주소로 변환하는 기술
  - 등장 배경
    - 주소 공간 부족
      - 인터넷 이용자의 증가로 인한 주소 공간 문제를 해결
    - IP 주소 비용 증가
      - IP 주소가 희귀해지면서 비용이 증가
    - 보안 우려의 증가
      - 네트워크가 커지면서 악성 사용자 증가
  - 1994년 5월 RFC 1631, “The IP Network Address Translator(NAT)”로 채택

네트워크 주소 변환 프로토콜

- NAT 장·단점
  - NAT의 장점
    - 공인 IP 주소 공유
      - 대량의 호스트가 소수의 공인 IP 주소를 공유하여 비용 절감과 IP 주소 공간 보존
    - 쉬운 확장
      - 로컬 네트워크 장비는 사설 IP 주소를 이용하기 때문에 확장에 용이
    - 인터넷 서비스 제공자(ISP) 선택의 유연성
      - 기관에서 공인 IP 주소만 바꾸면 되기 때문에 ISP를 변경하는 것이 용이
      - 네트워크의 모든 클라이언트 장비의 주소를 다시 부여할 필요 없음
    - 보안 강화
      - 외부에서는 공인 IP 주소만 보고 내부의 사설 IP 주소를 알 수 없기 때문에 직접 접근이 어려움

네트워크 주소 변환 프로토콜

- NAT 장·단점
  - NAT의 단점
    - 복잡성
      - 네트워크를 구성하고 관리하는 데 있어 하나의 추가적인 시스템이기 때문에 관리하기 복잡함
    - 공인 IP 주소 부족으로 인한 문제
      - 호스트에는 공인 IP 주소가 없기 때문에 일부 애플리케이션 기능 사용 불가
      - 공격자로부터 호스트를 보호하지만 정당하게 접근하는 것도 어려워질 수 있음
    - 보안 프로토콜 문제
      - NAT는 IP 패킷의 헤더 필드만을 수정하기 때문에 헤더의 변조를 탐지하도록 설계된 IPsec과의 호환성 문제

네트워크 주소 변환 프로토콜

- NAT 주소 용어
  - 네트워크 장비의 위치를 식별하는 주소
    - 내부 주소(Inside address)
      - 내부 네트워크에 속한 장비의 주소
    - 외부 주소(Outside address)
      - 외부 네트워크에 속한 장비의 주소
  - 특정 네트워크에서 표현되는 주소
    - 로컬 주소(Local address)
      - 내부 네트워크에서 표현되는 주소
    - 전역 주소(Global address)
      - 외부 네트워크에서 표현되는 주소

네트워크 주소 변환 프로토콜

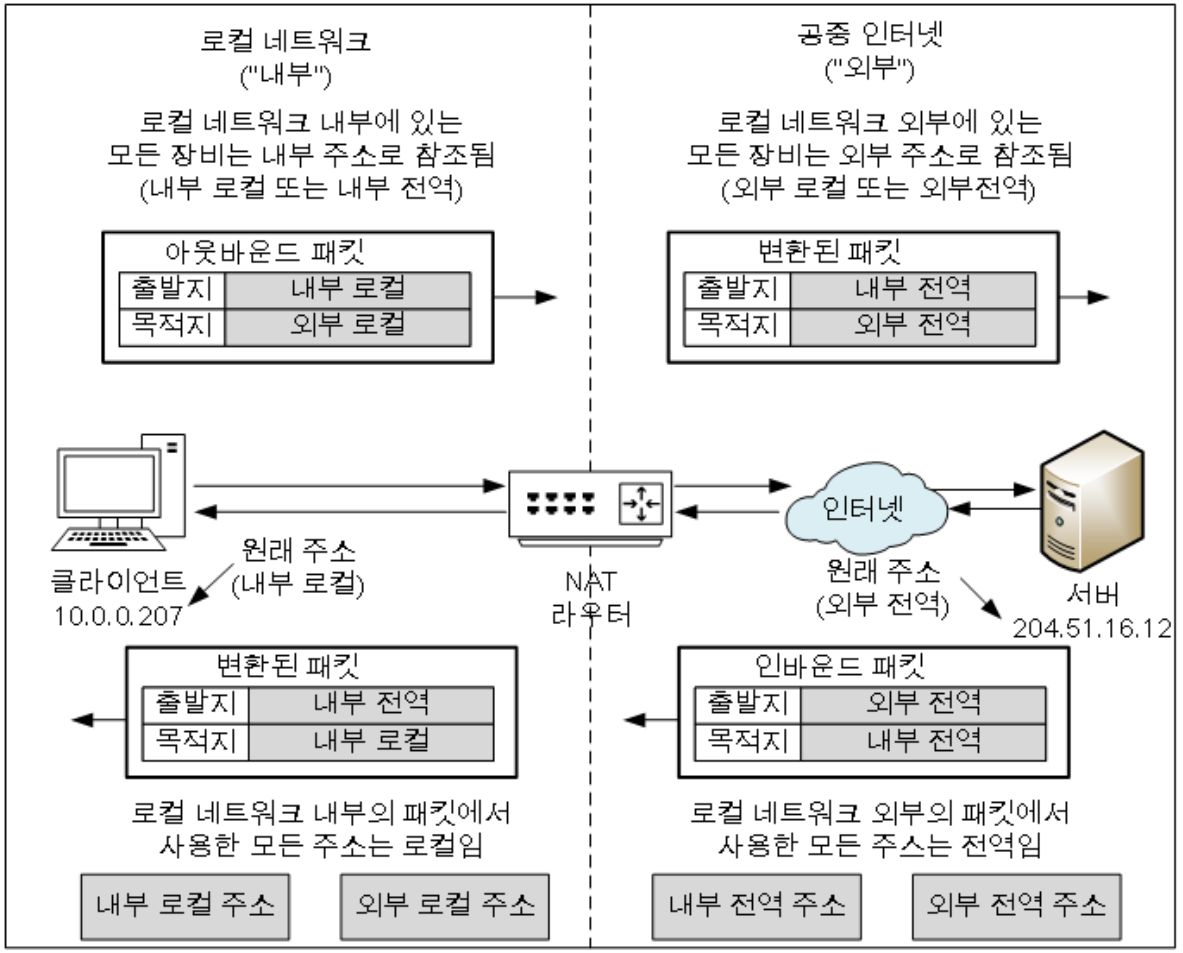
- NAT 주소 용어
  - NAT 내부/외부/로컬/전역 표

내부 로컬 주소 (Inside local address)	내부 전역 주소 (Inside global address)	외부 로컬 주소 (Outside local address)	외부 전역 주소 (Outside global address)
내부 네트워크에서 사용하는 장비의 주소 e.g., 사설 IP	내부 장비의 주소를 외부 네트워크에서 표현하기 위해 변환된 주소	외부 장비의 주소를 내부 네트워크에서 표현하기 위해 변환된 주소	공중 네트워크에서 사용하는 외부 장비의 주소 e.g., 공인 IP

    - 내부 또는 외부 장비의 주소를 로컬 표현에서 전역 표현으로, 또는 그 역으로 변환

네트워크 주소 변환 프로토콜

- NAT 주소 용어
  - NAT 내부/외부/로컬/전역 그림



네트워크 주소 변환 프로토콜

- NAT 주소 매핑
  - NAT 라우터는 주소 변환 방법을 지시하는 변환 테이블을 관리
    - 변환 테이블
      - 내부 장비의 내부 로컬 주소를 내부 전역 주소로 매핑하는 정보를 포함
      - 필요한 경우 외부 전역 주소와 외부 로컬 주소간 매핑 정보도 포함

네트워크 주소 변환 프로토콜

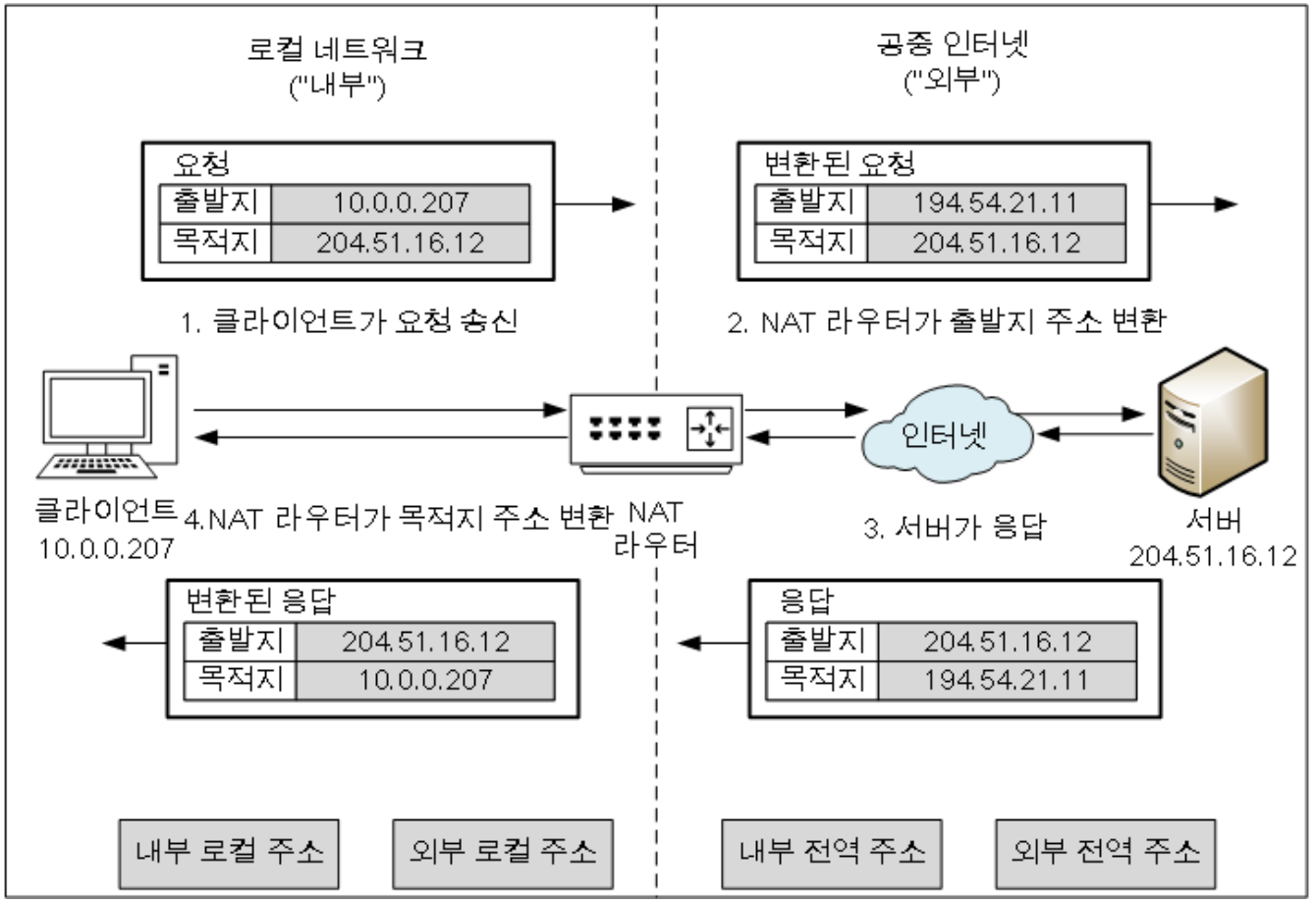
- NAT 주소 매핑
  - 정적 매핑(Static mapping)
    - 고정된 주소 관계를 의미
    - 외부 네트워크에 항상 동일한 공인 IP로 표현되어야 할 장비에 적합
      - e.g., 웹 서버, 메일 서버 등
  - 동적 매핑(Dynamic mapping)
    - 풀(Pool)에 있는 주소 중 하나씩 필요할 때마다 즉시 생성
      - 사용이 만료되면 반환

네트워크 주소 변환 프로토콜

- NAT의 구체적인 동작 방식
  - NAT 단방향(전통적/아웃바운드) 동작
    - 내부 네트워크 장비가 외부 네트워크 장비로 요청할 경우
      - 외부로 나가는 패킷의 출발지 주소 변환
      - 내부로 들어오는 패킷의 목적지 주소 변환

네트워크 주소 변환 프로토콜

- NAT의 구체적인 동작 방식
  - NAT 단방향(전통적/아웃바운드) 동작
    - 동작 과정 그림

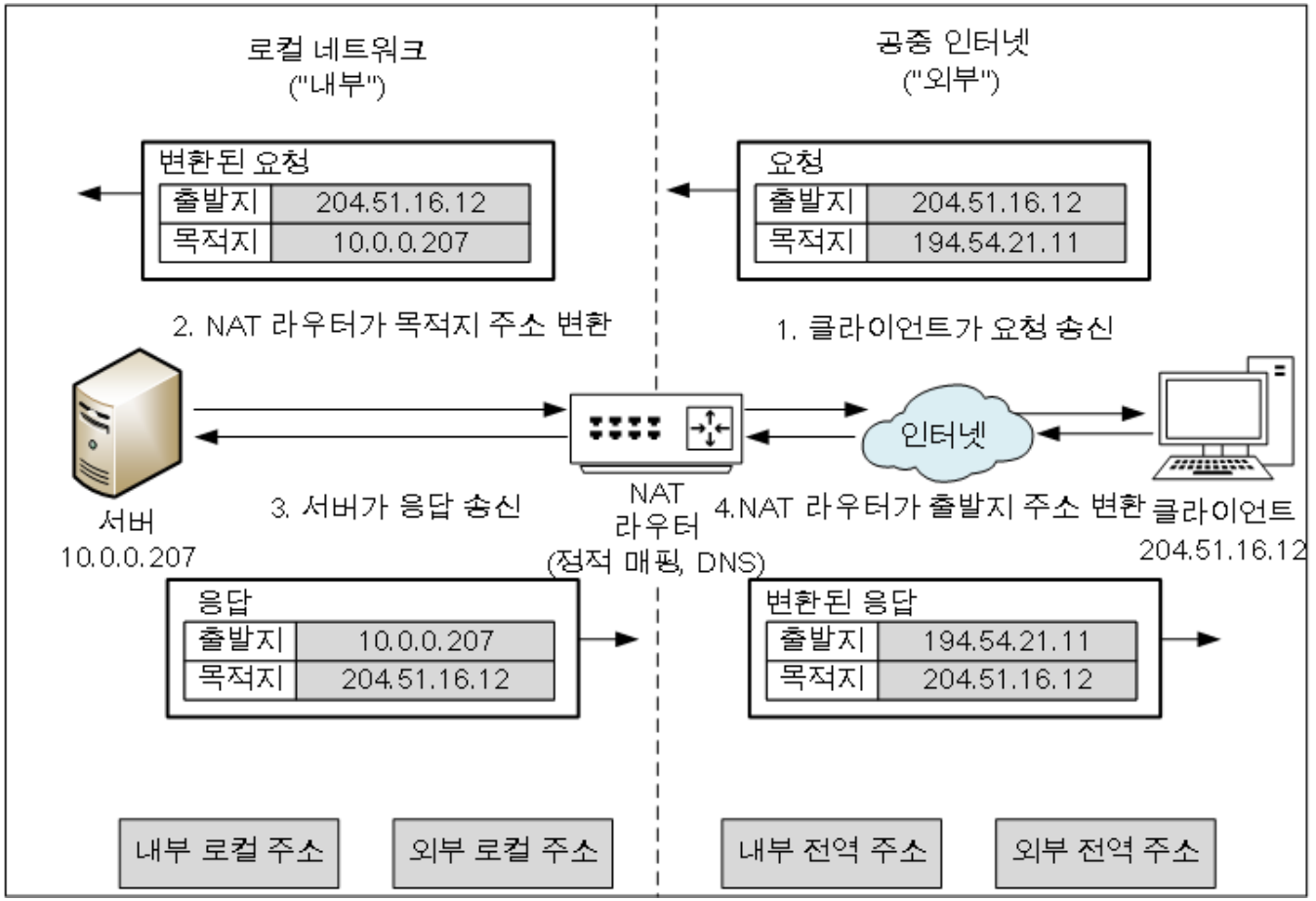


네트워크 주소 변환 프로토콜

- NAT의 구체적인 동작 방식
  - NAT 양방향(Two-Way/인바운드) 동작
    - 외부 네트워크 장비가 내부 네트워크 장비로 요청할 경우
      - 외부에서 들어오는 패킷의 목적지 주소 변환
      - 내부에서 나가는 패킷의 출발지 주소 변환
    - 외부 장비는 내부 네트워크의 사설 장비에게 패킷을 전송할 수 없음
      - 내부 네트워크의 로컬 라우터로 패킷을 전달할 방법이 없기 때문
      - 사설 장비의 내부 전역 주소를 알아야 함
    - 두 가지 해결 방안
      1. 정적 매핑
         - 내부 장비의 전역 주소를 외부에 알림
      2. DNS(Domain Name System) 매핑
         - IP 주소가 아닌 이름을 이용하여 해당 주소를 변환

네트워크 주소 변환 프로토콜

- NAT의 구체적인 동작 방식
  - NAT 양방향(Two-Way/인바운드) 동작
    - 동작 과정 그림

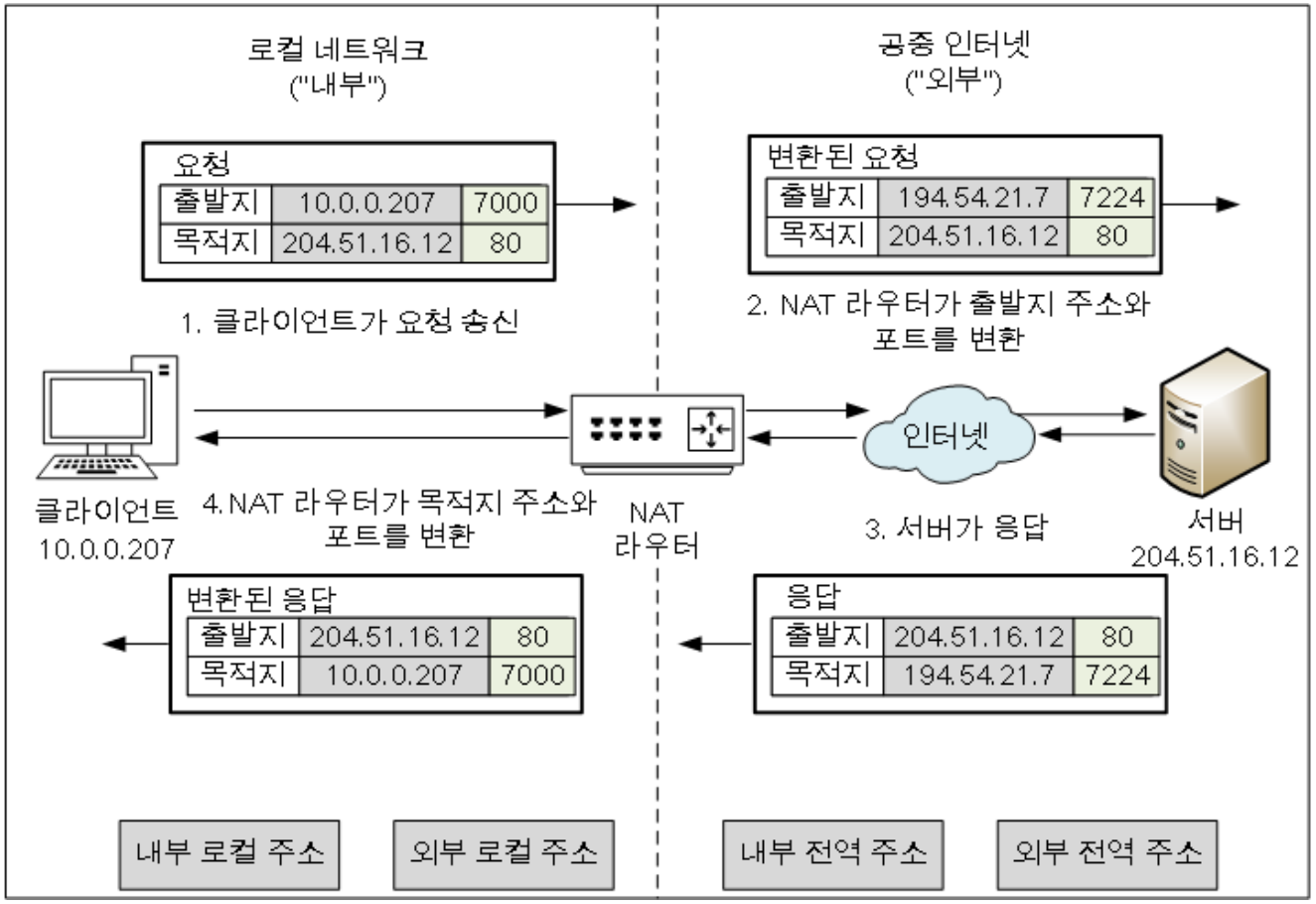


네트워크 주소 변환 프로토콜

- NAT의 구체적인 동작 방식
  - NAT 포트 기반(과부하) 동작
    - IP 주소와 포트 번호를 변환하는 방식
      - IP 주소와 포트 번호를 같이 매핑하여 여러 개의 사설 장비들이 내부 전역 주소 공유하여 동시에 인터넷을 접속할 수 있도록 함
    - 사용 가능한 내부 전역 주소가 남아 있지 않은 경우
      - 외부로 나가는 패킷의 출발지 주소와 포트 번호 변환
      - 내부로 들어오는 패킷의 목적지 주소와 포트 번호 변환

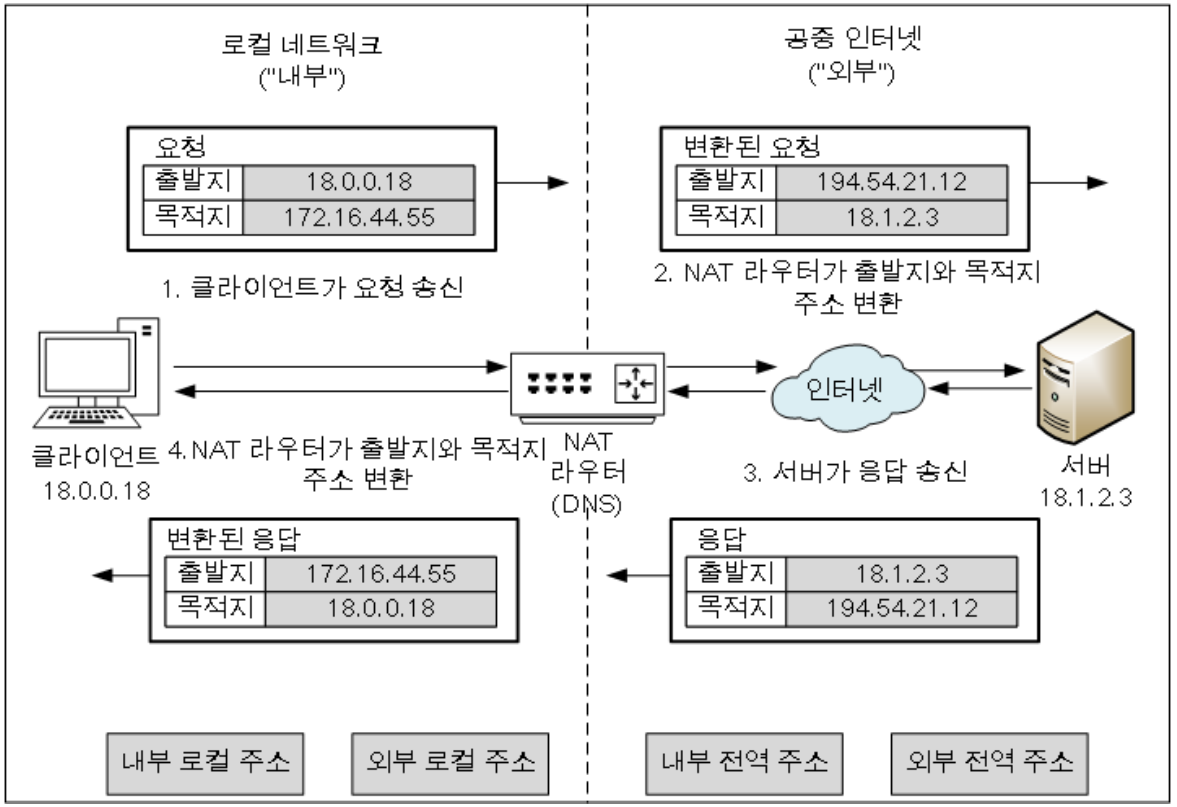
네트워크 주소 변환 프로토콜

- NAT의 구체적인 동작 방식
  - NAT 포트 기반(과부하) 동작
    - 동작 과정 그림



네트워크 주소 변환 프로토콜

- NAT의 구체적인 동작 방식
  - NAT 중복/2회 NAT 동작
    - 내부 네트워크 주소와 외부 네트워크 주소가 중복될 경우
      - 내부로 들어오거나 외부로 나가는 패킷의 출발지 주소와 목적지 주소 모두를 변환
    - 동작 과정 그림



네트워크 주소 변환 프로토콜

- NAT 호환성과 특수 처리
  - 주요 문제와 요구 사항
    - 주소나 포트 번호 변경에 의한 파급 효과
      - TCP와 UDP 체크섬 재계산
        - 헤더의 IP 주소 변경 시 IP 헤더의 체크섬을 다시 계산해야 함
      - IPsec과의 호환성 문제
    - 인터넷 제어 메시지 프로토콜(ICMP, Internet Control Message Protocol) 조작
      - ICMP 메시지는 패킷의 원본 IP 헤더를 포함
      - NAT는 ICMP 메시지를 조사하여 필요에 맞게 주소를 변환해야 함

목 차

- 보 충
  - IP 라우팅과 멀티캐스팅
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

IP Security 프로토콜

- IPsec(Internet Protocol Security)
  - IP 네트워크에 보안을 제공하는 서비스와 프로토콜 모음
  - 등장 배경
    - IP 계층에서 TCP/IP 프로토콜과 애플리케이션의 안전을 보장하는 기능 부재로 인해 등장
  - 기능
    - 데이터 암호화
    - 메시지의 무결성을 인증
    - 재전송 공격(Replay attack)으로부터 보호
    - 보안 요구에 맞는 보안 알고리즘과 키 협상
    - 두 가지 보안 모드
      - 전송(Transport) 모드
      - 터널(Tunnel) 모드

IP Security 프로토콜

- IPsec 프로토콜 슈트
  - 핵심 프로토콜 표

IPsec 핵심 프로토콜	기능
IPsec 인증 헤더 (AH, Authentication Header)	데이터 무결성 및 인증 제공 재전송 공격에 대한 보호 기능 제공
보안 페이로드 캡슐화 (ESP, Encapsulating Security Payload)	데이터 기밀성, 무결성, 인증 제공

  - 보조 구성 요소 표

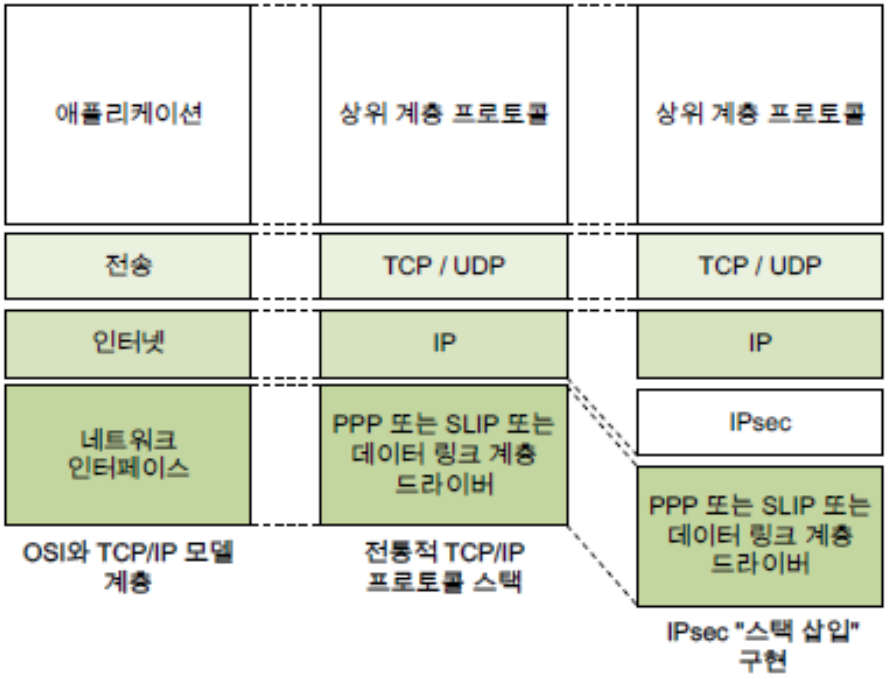
보조 구성 요소	기능
암호화/해시 알고리즘	DES(Data Encryption Standard) MD5(Message Digest 5)
보안 정책, 연관, 관리 방법	장비간에 보안과 관련된 정보 교환
키 교환 프레임워크와 방법	인터넷 키 교환 (IKE, Internet Key Exchange)

IP Security 프로토콜

- IPsec 구현 방법 및 구조
  - 구현 방법
    - 종단 호스트 구현
      - 모든 호스트 장비에 구현하여 유연성과 보안성을 높임
      - 네트워크 종단간 모든 장비 사이를 보호
    - 라우터 구현
      - 비교적 소수의 라우터에 구현
      - 구현한 라우터 쌍 사이만 보호
      - 라우터와 로컬 호스트 사이의 연결은 보호되지 않음
    - 네트워크의 요구 사항에 따라 구현 방법 고려

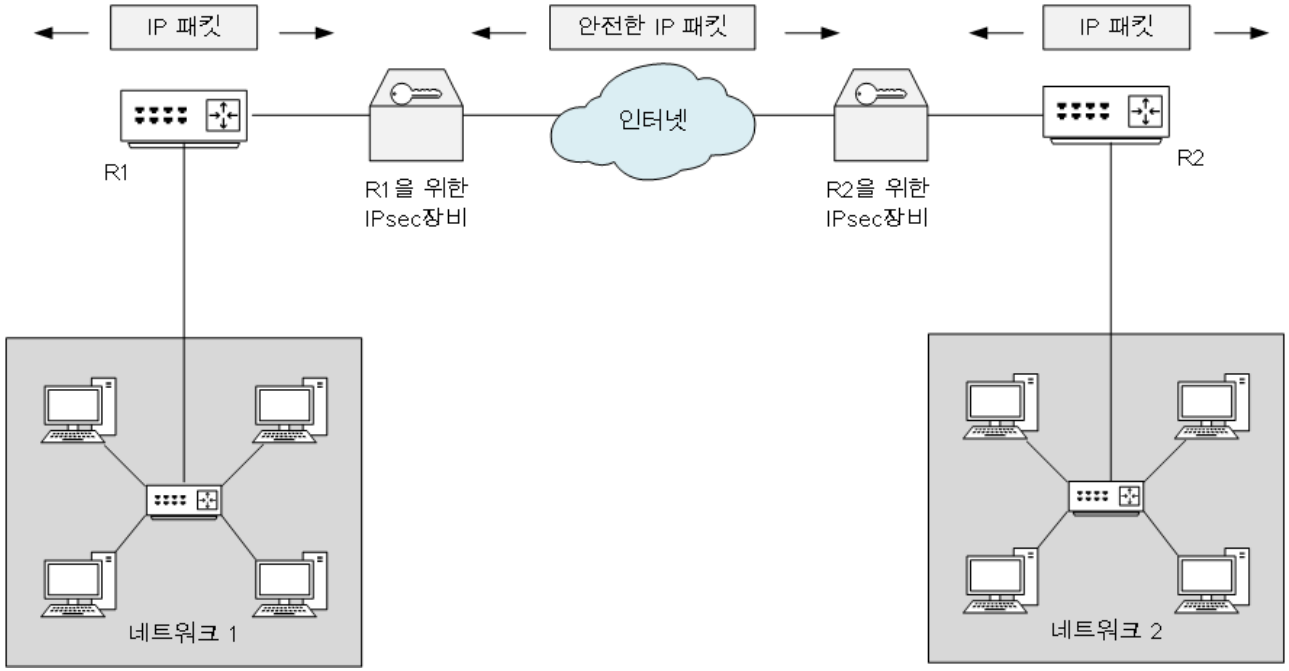
IP Security 프로토콜

- IPsec 구현 방법 및 구조
  - TCP/IP 프로토콜 스택과 결합하는 방법
    - 통합 구조
      - IPsec의 프로토콜과 기능을 IP 계층에 통합
      - 추가적인 하드웨어나 계층 불필요
      - IPv4의 경우, 각 장비의 IP 구현을 변경해야 함
    - 스택 삽입 구조(BITS, Bump In The Stack)
      - IP와 데이터 링크 계층 사이에 별도 구조 계층으로 존재
      - 데이터 링크 계층에 가기 전에 IP 패킷을 가로채 보안 기능을 덧붙인 뒤 전달



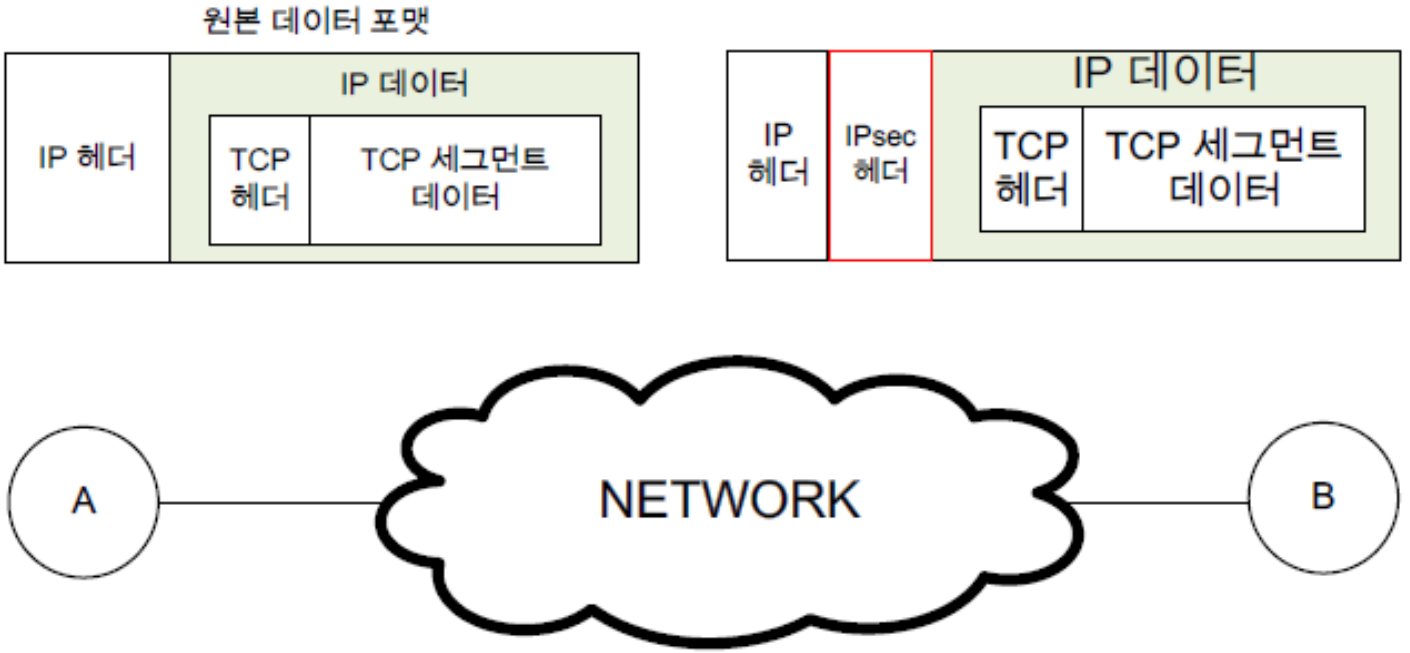
IP Security 프로토콜

- IPsec 구현 방법 및 구조
  - TCP/IP 프로토콜 스택과 결합하는 방법
    - 라인 삽입 구조(BITW, Bump In The Wire)
      - IPsec 서비스를 제공하는 하드웨어 장비를 추가
        - 외부로 나가는 패킷을 가로채 IPsec 보호 기능 추가하여 송신
        - 내부로 들어오는 패킷의 IPsec 관련 헤더 제거



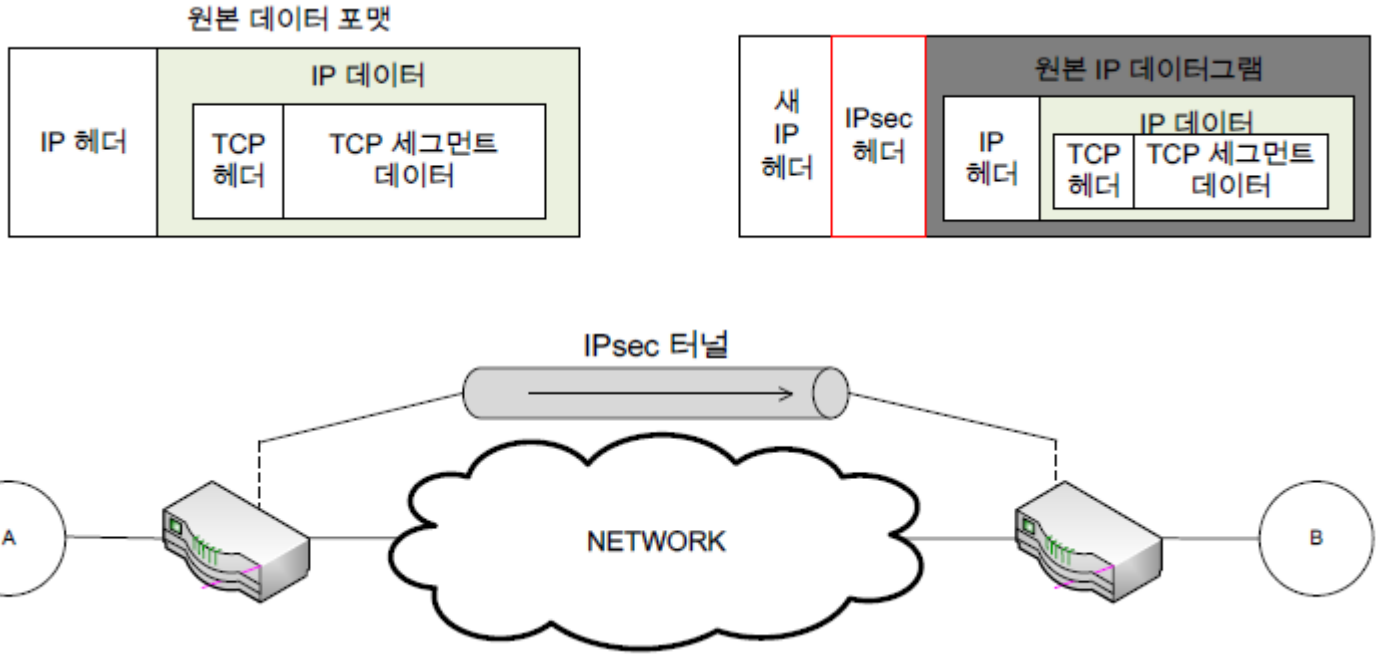
IP Security 프로토콜

- IPsec 모드
  - 전송 모드(Transport mode)
    - 전송 계층에서 내려온 패킷을 보호
    - IP 헤더는 보호되지 않고 IP 페이로드만 보호
    - 통합 구조와 종단 호스트 간에 주로 사용



IP Security 프로토콜

- IPsec 모드
  - 터널 모드(Tunnel mode)
    - IP 헤더를 포함한 패킷 전체를 보호
    - 추가적인 캡슐화 진행
      - 원본 IP 패킷이 AH와 ESP 헤더를 포함하는 새로운 IP 패킷으로 캡슐화



IP Security 프로토콜

- IPsec 보안 구성 요소
  - 보안 정책(SP, Security Policy)
    - 장비가 수신하는 서로 다른 패킷에 보안을 어떻게 제공할지에 대한 전반적인 지침을 기술
    - 보안 정책 데이터베이스(SPD, Security Policy Database)에 저장됨
  - 보안 연관(SA, Security Association)
    - 각 장비 사이에 안전한 통신을 하기 위해 사용하는 보안 방법을 명시한 정보
    - 보안 연관 데이터베이스(SAD, Security Association Database)에 저장됨

IP Security 프로토콜

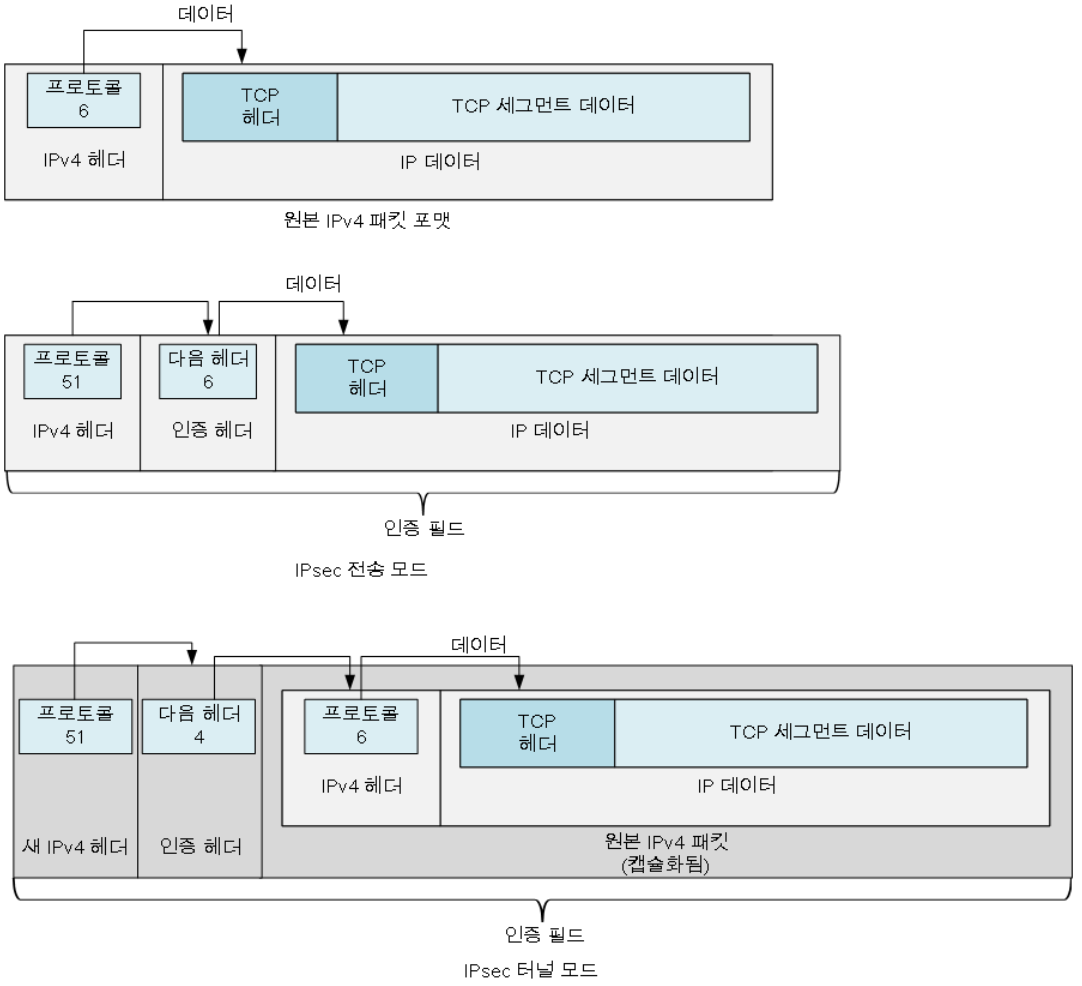
- IPsec 보안 구성 요소
  - 보안 연관 트리플과 보안 인자 색인
    - SA는 트리플이라고 불리는 세 개의 인자 모음으로 정의
      - 보안 인자 색인(SPI, Security Parameters Index)
        - 연결된 장비의 특정 SA를 식별하기 위해 선택된 32비트 숫자
        - 메시지 수신자가 패킷에 어떤 SA가 적용되는지 파악하는 데 쓰임
      - IP 목적지 주소
        - SA가 수립된 장비의 주소
      - 보안 프로토콜 식별자
        - AH와 ESP 보안 연관을 식별
        - 둘 다 사용하는 경우, 각각 별도의 SA를 지정

IP Security 프로토콜

- IPsec 인증 헤더(AH, Authentication Header)
  - 개요
    - AH 헤더 위치
      - 모드와 버전에 따라 적절한 위치에 삽입
    - 패킷 전체 또는 일부분에 대해 인증을 제공
    - 해시 알고리즘 사용
      - MD5, SHA-1
    - 계산된 무결성 검사 값(ICV, Integrity Check Value)을 헤더에 추가하여 전송
    - 메시지의 무결성 보장
    - 재전송 공격에 대한 보호 기능 제공

IP Security 프로토콜

- IPsec 인증 헤더(AH)
  - AH를 포함하는 IP 패킷 포맷
    - 전송 모드
      - 원본 IP 패킷의 헤더와 페이로드 사이에 AH를 추가하여 캡슐화
    - 터널 모드
      - 캡슐화된 IP 패킷에 AH를 추가하여 새로운 IP 패킷으로 캡슐화



IP Security 프로토콜

- IPsec 인증 헤더(AH)
  - AH 포맷

필드 이름	크기 (바이트)	설명
다음 헤더	1	AH 다음에 오는 헤더의 프로토콜 번호
페이로드 길이	1	인증 헤더 자체의 길이
예약됨	2	쓰이지 않음, 0으로 설정
SPI	4	목적지 주소와 보안 프로토콜 유형(AH)과 함께 패킷에 쓰이는 보안 연관(SA)을 식별
순서 번호	4	패킷이 송신될 때마다 값을 증가시켜 재전송 공격을 방지
인증 데이터	가변적	해시 알고리즘의 계산 결과인 무결성 검사 값(ICV)을 포함

IP Security 프로토콜

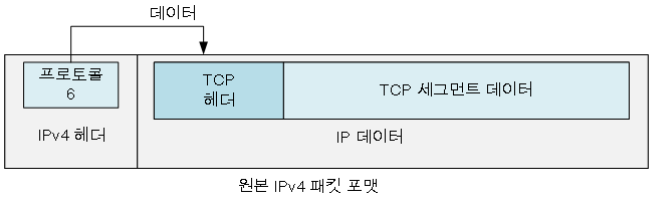
- IPsec 보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)
  - 개요
    - IP 패킷을 암호화하여 메시지의 기밀성 보장
      - 암호화 알고리즘과 키를 사용
        - e.g., AES, DES, 3DES
    - 수신 측에서 인터넷 키 교환(IKE, Internet Key Exchange)으로 미리 교환한 Key 값을 이용하여 데이터를 복호화

IP Security 프로토콜

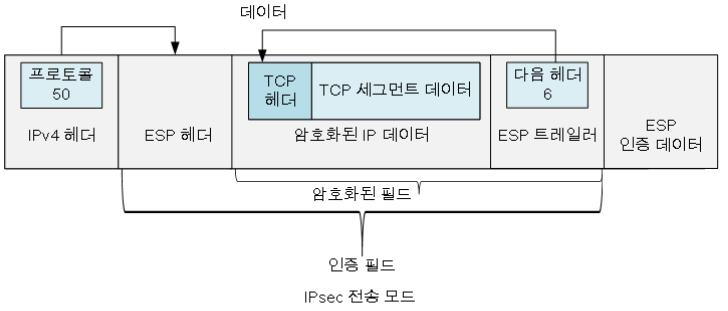
- IPsec 보안 페이로드 캡슐화(ESP)
  - ESP 필드의 세 가지 구성 요소
    1. ESP 헤더
       - 보안 인자 색인(SPI)과 순서 번호(Sequence number)라는 두 필드를 포함
    2. ESP 트레일러
       - 암호화된 데이터를 패딩과 패딩 길이 필드를 이용해 32비트 경계에 맞춤
       - ESP의 다음 헤더 필드 포함
    3. ESP 인증 데이터
       - AH 프로토콜과 유사한 방식으로 계산되는 ICV 값을 포함

IP Security 프로토콜

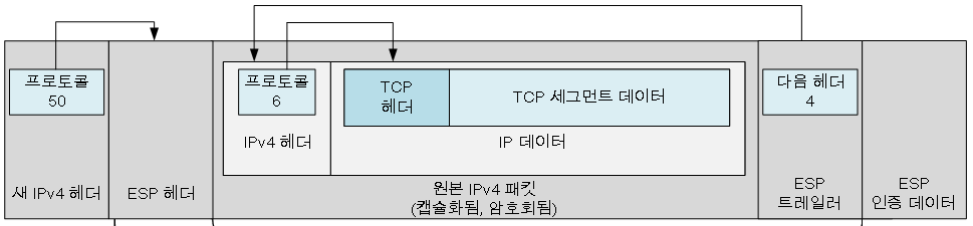
- IPsec 보안 페이로드 캡슐화(ESP)
  - ESP를 포함하는 IP 패킷 포맷
    - 전송 모드
      - ESP 헤더
        - 암호화된 데이터 앞에 위치
        - 모드와 버전에 따라 적절한 위치에 삽입
      - ESP 트레일러, 인증 데이터
        - 암호화된 데이터 위에 위치
    - 터널 모드
      - 원본 IP 패킷이 ESP 헤더와 트레일러, 인증 데이터로 둘러싸여있음



원본 IPv4 패킷 포맷



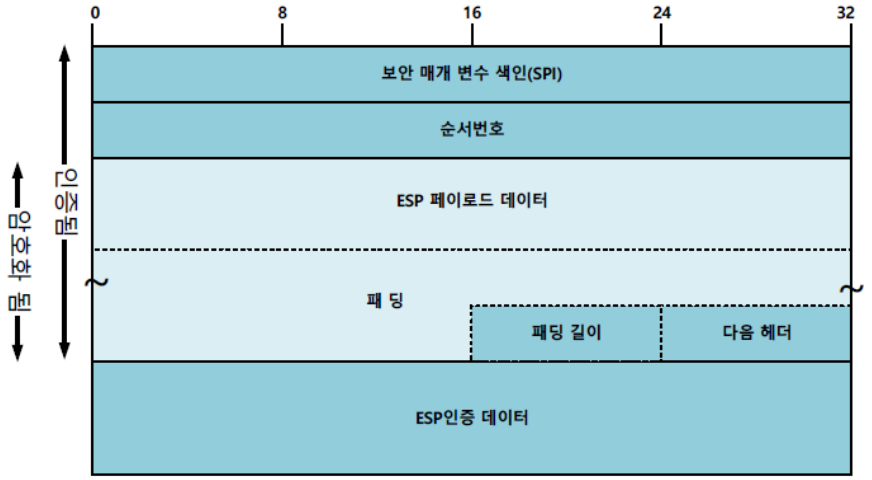
IPsec 전송 모드



IPsec 터널 모드

IP Security 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
  - ESP 포맷



구간	필드 이름	크기 (바이트)	설명	암호화 범위	인증 범위
ESP 헤더	SPI	4	32비트 값으로, 패킷에 쓰이는 보안 연관(SA)을 식별		
	순서 번호	4	패킷이 송신될 때마다 값을 증가시켜 재전송 공격을 방지		
페이로드	페이로드	가변적	쓰이지 않음, 0으로 설정		
ESP 트레일러	패딩	가변적 (0 ~ 255)	암호화 또는 정렬을 위해 추가적인 패딩 바이트가 포함됨		
	패딩 길이	1	패딩 필드의 바이트 수		
	다음 헤더	1	패킷에서 다음 헤더의 프로토콜 번호를 포함		
ESP 인증 데이터		가변적	해시 알고리즘의 계산 결과인 무결성 검사 값(ICV)을 포함		

IP Security 프로토콜

- IPsec 인터넷 키 교환(IKE, Internet Key Exchange)
  - 개요
    - 세 개의 다른 프로토콜의 기능을 결합한 혼성 프로토콜
      - 보안 관련 설정들을 생성, 협상, 관리
    - 장비가 정보를 교환할 때 안전한 통신을 보장
      - IPsec 지원 장비가 SA를 교환하는 방식으로 동작
    - IPsec 표준에 추가 기능, 유연성 및 구성 용이성을 제공

IP Security 프로토콜

- IPsec 인터넷 키 교환(IKE)
  - IKE를 구성하는 세 가지 프로토콜
    1. ISAKMP(Internet Security Association and Key Management Protocol)
       - 두 가지 키 교환 프로토콜의 기능을 결합한 범용 프로토콜
         - 인증 및 키 교환을 위한 구조를 제공하지만 실제 키 교환을 정의하지 않음
    2. OAKLEY 키 교환 프로토콜
       - 키 교환 모드를 정의
       - 구체적인 키 교환 방법을 설명
       - IKE의 키 교환 절차의 대부분은 OAKLEY 기반
    3. SKEME 키 교환 프로토콜
       - OAKLEY와는 다른 키 교환 방법을 설명
         - e.g., 공개키 암호의 키 갱신 등
       - IKE는 SKEME의 일부 기능을 이용

IP Security 프로토콜

- IPsec 인터넷 키 교환(IKE)
  - IKE 동작
    - ISAKMP 구조 내에서 동작
      - 1단계
        - 두 장비가 정보를 어떻게 안전하게 교환할지에 동의하는 준비 단계
        - 협상을 통해 ISAKMP 자체를 위한 ISKMP SA를 생성
        - ISAKMP SA에 포함되는 속성
          - 암호화 알고리즘
          - 해시 알고리즘
          - 인증 방법
          - 키 교환 방법
      - 2단계
        - 생성한 ISKMP SA를 이용하여 기타 보안 프로토콜을 위한 SA를 생성
        - AH와 ESP 프로토콜을 위한 SA의 인자를 협상

목 차

- 보 충
  - IP 라우팅과 멀티캐스팅
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

모바일 IP

- 개요
  - 등장 배경
    - 무선 LAN 기술이 도입되어 모바일 컴퓨팅이 증가하면서 IP 주소 기반 지정 방법이 이동 장비를 지원하지 못함
      - IP 주소 내에는 네트워크 ID와 호스트의 IP 주소가 결합되어 있음
    - 네트워크 ID와 호스트 ID로 구별되는 IP 주소 체계에서 이동 장비가 선택할 수 있는 두 가지 방안
      1. 이동한 네트워크로 IP 주소 변경
         - 사람이 직접 관여하기 때문에 시간이 오래 걸림
         - 사용하던 모든 연결을 끊고 다시 연결해야 함
         - 변경한 IP 주소를 다른 장비에게 알리기 어려움
      2. IP 라우팅 방식 변경
         - 라우팅 테이블 항목 수가 많아져 관리하기 어려움

모바일 IP

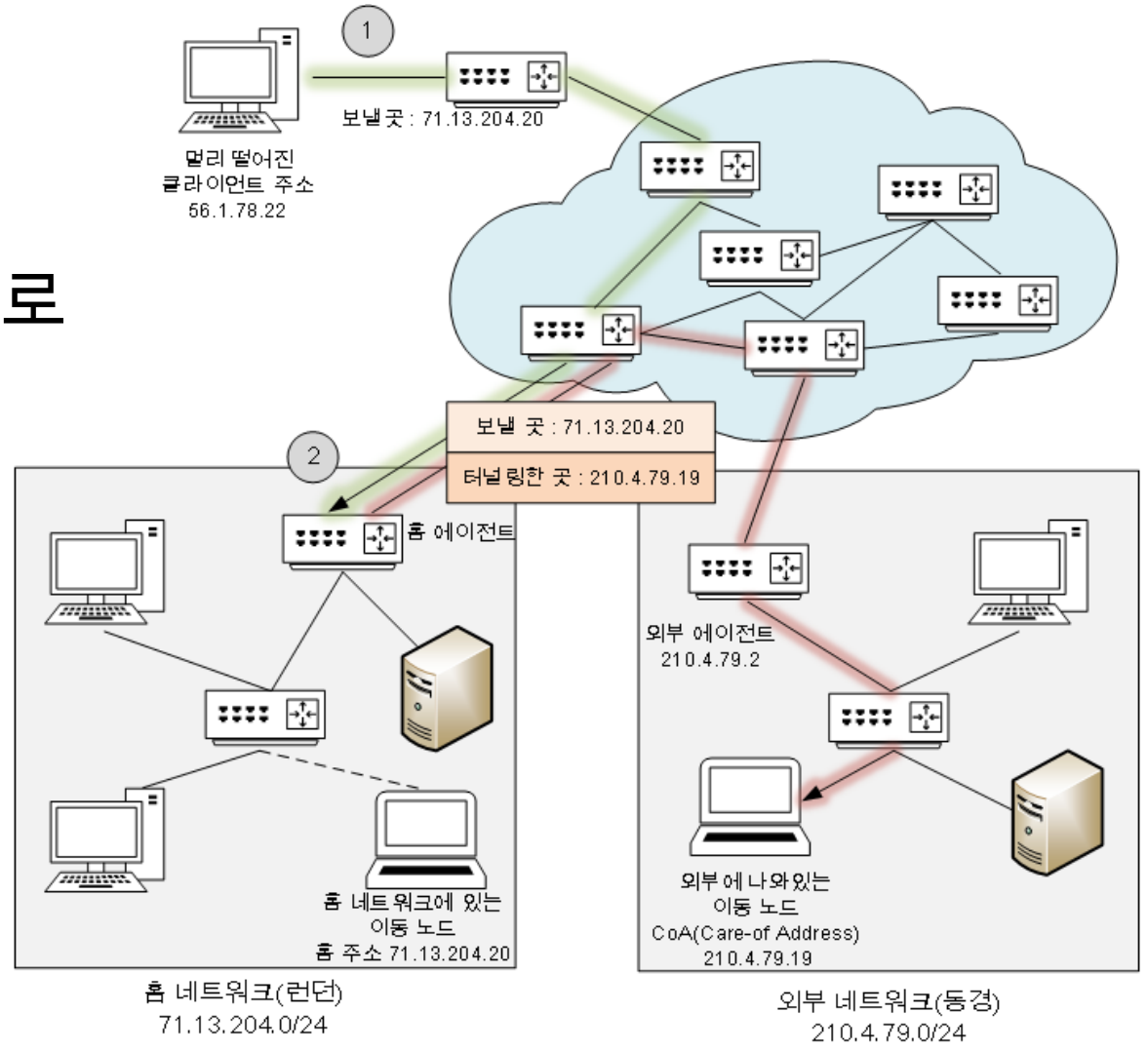
- 개요
  - 해결책
    - 이동성 지원 프로토콜(모바일 IP)을 정의하여 IP에 추가시켜 이동성 문제를 해결
    - 모바일 IP
      - 이동 장비의 홈 네트워크에 도착한 패킷을 이동 장비가 실제로 있는 네트워크로 전달하는 시스템

모바일 IP

- 모바일 IP 장비
  - 이동 장비
    - 네트워크를 이동하는 장비
  - 홈 에이전트(Home agent)
    - 이동 장비의 홈 네트워크의 라우터
    - 이동 장비가 받아야 할 패킷을 대신 받아 이동 장비에게 전달
  - 외부 에이전트(Foreign agent)
    - 이동 장비가 현재 위치하고 있는 네트워크의 라우터
    - 새로운 홈 네트워크의 역할을 수행
    - 모바일 IP 동작을 위해 이동 정보를 공유할 수 있음

모바일 IP

- 모바일 IP 동작 방식 그림
  - 홈 에이전트
    - 이동 장비의 원래 IP 주소로 도착한 패킷을 이동 장비의 현재 위치로 전달
    - 이동 장비에게 패킷을 직접 전달하거나 외부 에이전트를 통해 간접적으로 전달



모바일 IP

- 모바일 IP 기능
  - 에이전트 통신
    - 이동 장비는 에이전트가 보내는 광고 메시지를 통해 자신의 위치를 파악
    - 광고 메시지를 듣지 못할 시, 에이전트 요청 메시지 전송
  - 네트워크 위치 결정
    - 에이전트 발견 메시지 내용을 기반으로 자신의 위치 판단

모바일 IP

- 모바일 IP 기능
  - 장비가 외부 네트워크로 이동한 경우
    - CoA(Care of Address) 획득
      - 이동 장비는 CoA 임시 주소를 받음
      - 목적지로 패킷을 전달할 때 이외에는 사용하지 않음
    - 에이전트 등록
      - 이동 장비는 자신의 위치를 홈 에이전트에 등록하여 자신에게 오는 패킷을 대신 전달해달라고 요청
      - 외부 에이전트가 중개자로 개입할 수도 있음
    - 패킷 전달
      - 홈 에이전트가 대신 패킷을 받아 실제 이동 장비의 위치로 전달
      - CoA의 종류에 따라 직접 전달하거나 외부 에이전트에게 전달을 부탁할 수도 있음

모바일 IP

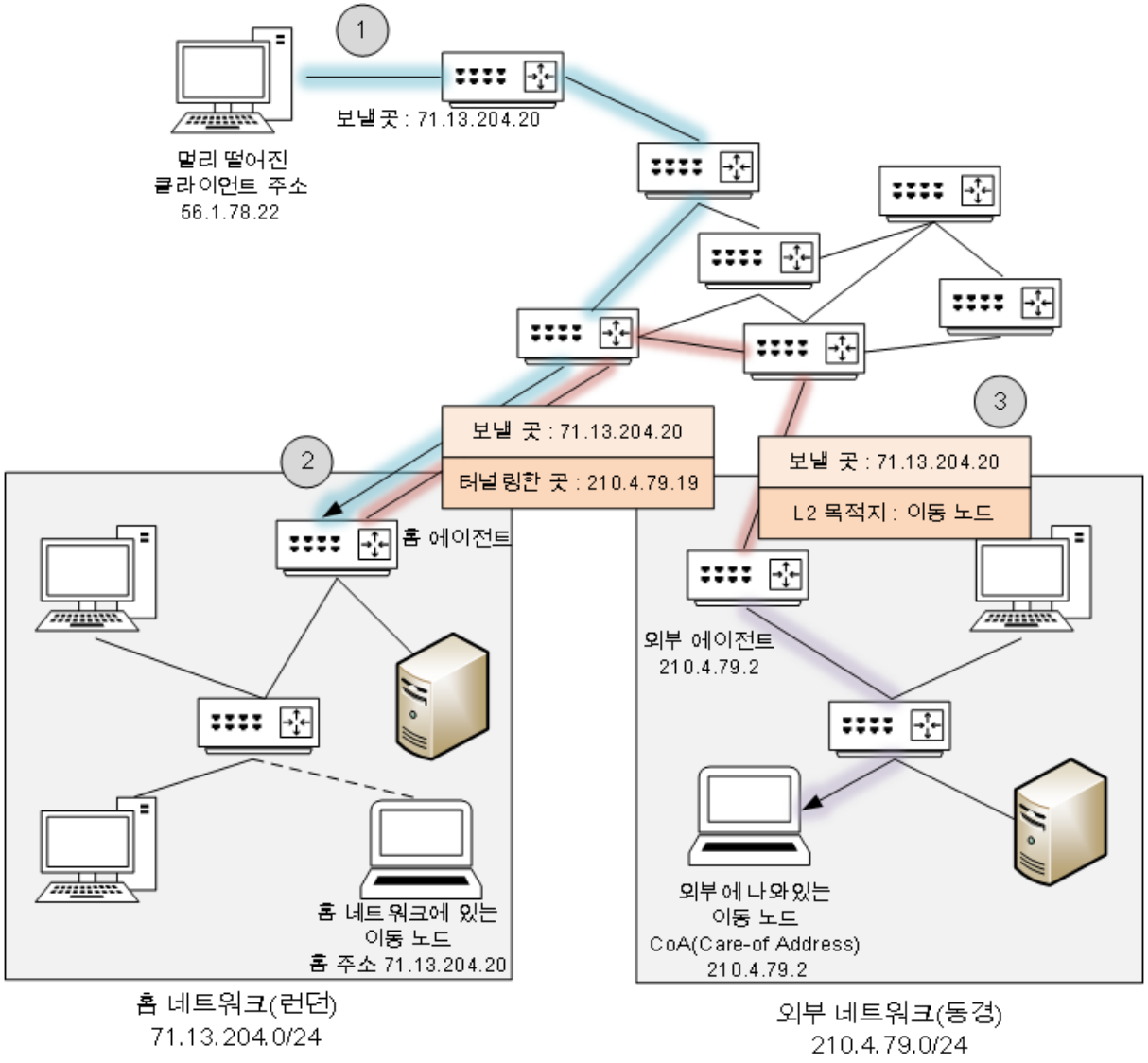
- 모바일 IP 주소
  - 홈 주소
    - 이동 장비에게 할당된 고정 IP 주소
      - 홈 네트워크에서 장비가 사용하는 주소
    - 패킷을 이동 장비에게 보낼 때 사용
  - CoA(Care of Address)
    - 이동 장비가 외부로 이동했을 때 사용하는 임시 주소
    - 32비트 IP 주소와 동일하지만 모바일 IP에서만 사용
      - IP 패킷을 목적지로 전달할 때 이외에는 사용하지 않음

모바일 IP

- 모바일 IP 주소
  - CoA 유형
    - 외부 에이전트 CoA
      - 외부 에이전트의 IP 주소 사용
      - 홈 에이전트가 CoA로 전달한 패킷은 외부 에이전트가 이동 장비에게 전달

모바일 IP

- 모바일 IP 주소
  - CoA 유형
    - 외부 에이전트 CoA
      - 동작 과정 그림

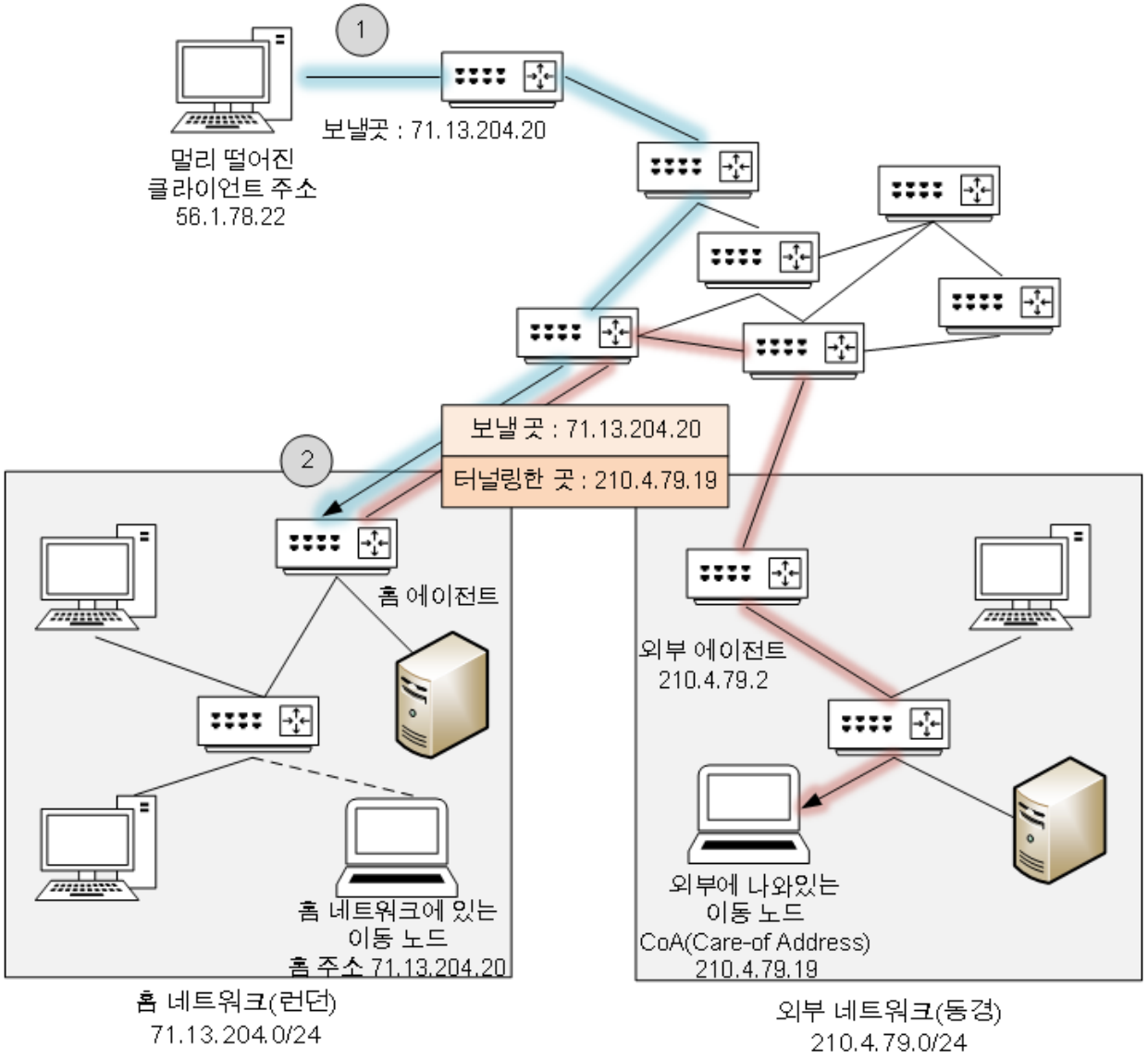


모바일 IP

- 모바일 IP 주소
  - CoA 유형
    - 공존 CoA(Co-Located Care of Address)
      - 이동 장비에 직접 할당된 주소
        - 직접 주소를 할당하거나 DHCP를 사용해서 자동으로 주소 할당
          - 동적 호스트 구성 프로토콜 (DHCP, Dynamic Host Configuration Protocol)
          - 자동 IP 할당 기법
      - 홈 에이전트가 패킷을 직접 이동 장비에게 전달

모바일 IP

- 모바일 IP 주소
  - CoA 유형
    - 공존 CoA
      - 동작 과정 그림



모바일 IP

- 모바일 IP 주소
  - CoA 유형에 따른 차이
    - 외부 에이전트 CoA
      - 외부 에이전트가 있는 경우
      - 외부 네트워크에 있는 모든 이동 장비들이 같은 외부 CoA를 사용
      - 각자 다른 IP 주소를 가질 필요가 없음
    - 공존 CoA
      - 외부 에이전트가 없는 경우
      - 모바일 IP 기능이 없는 네트워크를 지날 때에도 CoA 사용 가능
      - 각 장비가 외부 네트워크에서도 유일한 IP 주소를 가져야 함

모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 발견 과정
    - 이동 장비가 자신의 위치를 판단하고 홈이나 외부 에이전트와의 관계를 유지하기 위한 과정

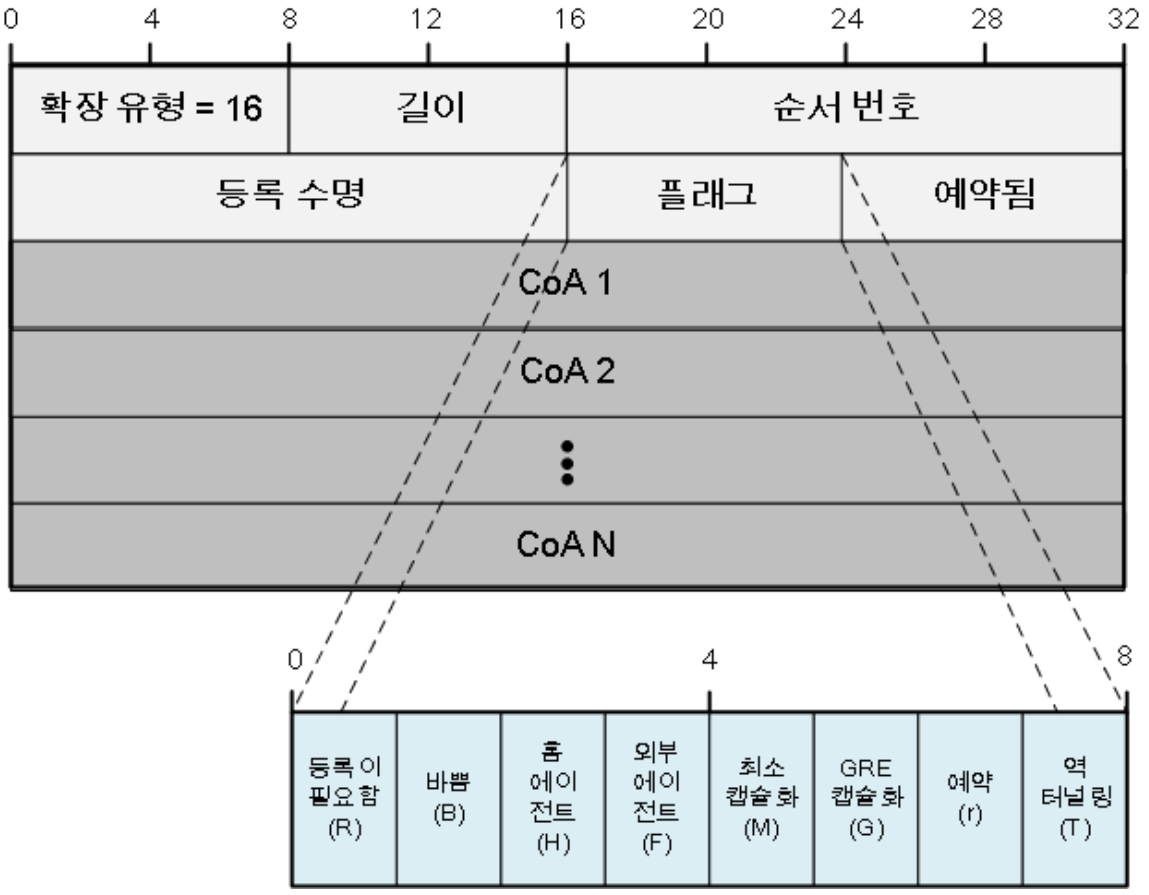
1. 에이전트/장비 통신
   - 에이전트 광고 메시지를 사용하여 주기적으로 자신의 존재를 알림
   - 에이전트 광고 메시지를 받지 못했을 때, 직접 에이전트 요청 메시지 전송
2. 현재 위치 발견
   - 이동 장비의 위치를 파악
3. CoA 할당
   - 이동 장비가 사용할 CoA 할당

모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고와 요청 메시지
    - 에이전트 광고(Agent advertisement) 메시지
      - 모바일 IP 에이전트로 활동할 수 있는 라우터가 정기적으로 전송
      - 모바일 IP 관련 정보와 하나 이상의 확장을 포함하는 라우터 광고 메시지로 구성됨
      - 이동 에이전트 광고(Mobility agent advertisement) 확장
        - 에이전트가 모바일 IP 기능을 갖추었다는 것을 알림
      - 접두사 길이(Prefix length) 확장
        - CoA 주소 내 네트워크 ID를 알림
      - 1 바이트 패딩(One byte padding) 확장
        - 메시지 길이를 짝수로 패딩

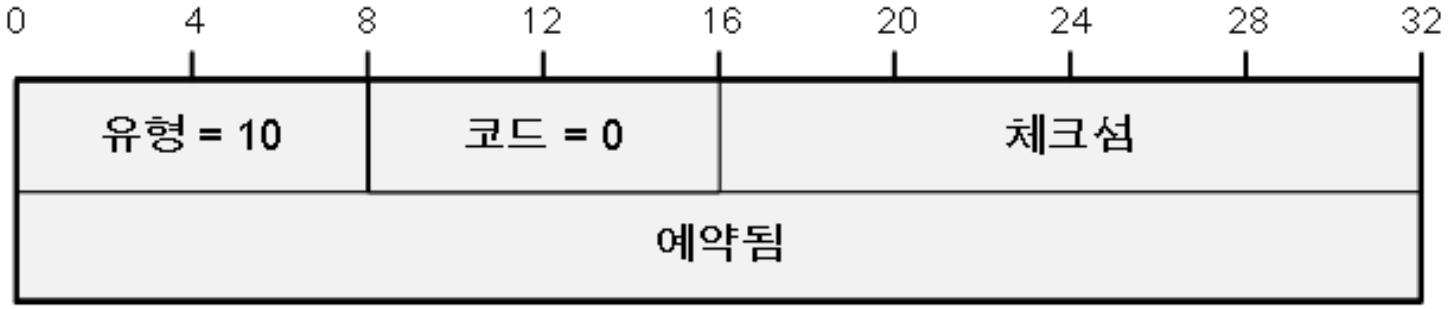
모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고와 요청 메시지
    - 에이전트 광고(Agent advertisement) 메시지
      - 메시지 포맷



모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고와 요청 메시지
    - 에이전트 요청(Agent solicitation) 메시지
      - 모바일 IP 장비가 홈 에이전트에게 광고를 전송해달라고 요청
      - 메시지 포맷



모바일 IP

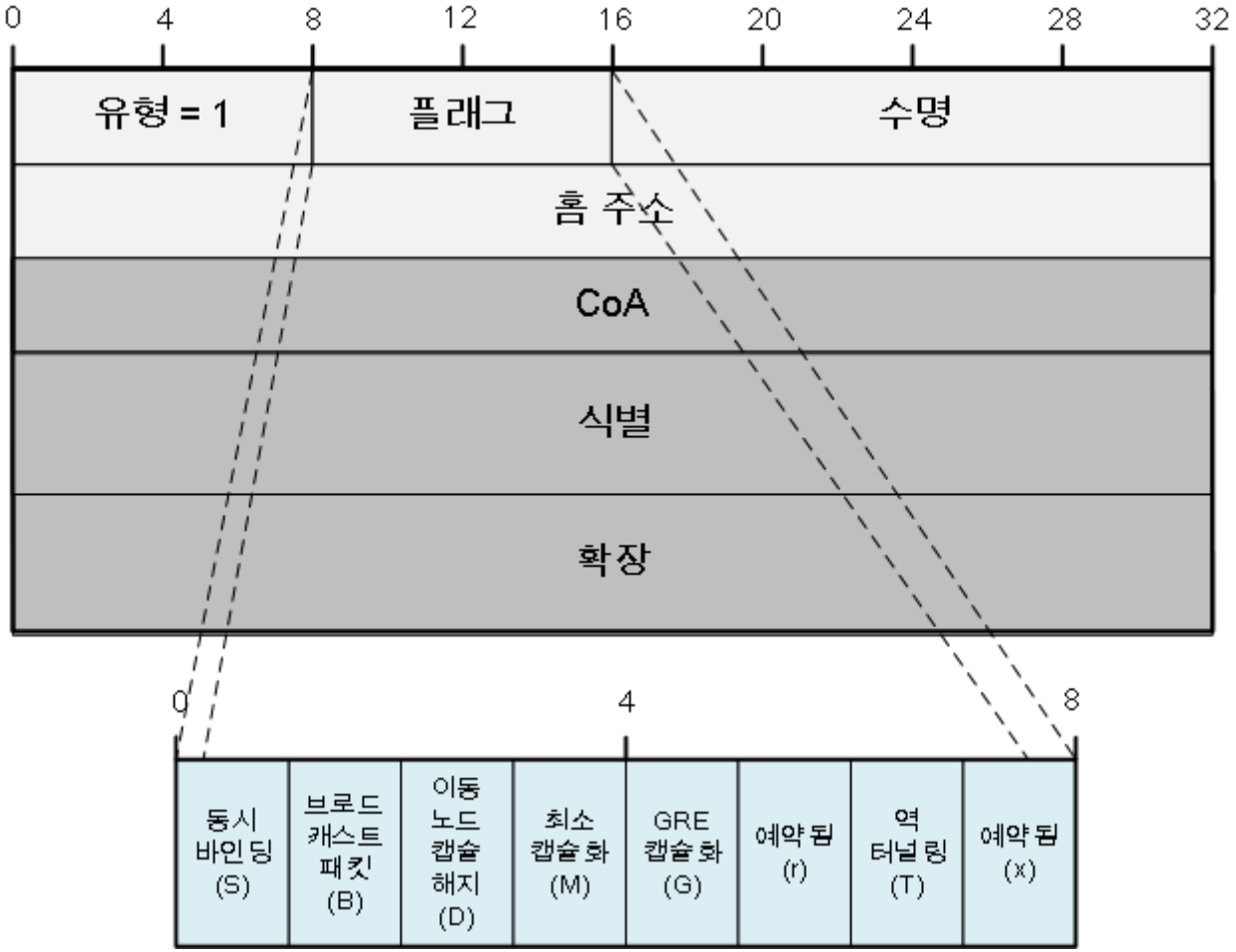
- 모바일 IP 에이전트 등록
  - 홈 에이전트 등록(Home agent registration)
    - 이동 장비가 홈 에이전트와 통신을 하면서 필요한 정보와 지시를 주고 받는 과정
  - 이동 장비 등록 이벤트
    - 등록 이동
      - 장비가 외부 네트워크에 도착하면 등록을 시작
    - 등록 해제
      - 다시 홈 네트워크로 돌아오면 전달을 취소하는 과정
    - 재등록
      - 다른 외부 네트워크로 이동하거나 CoA가 바뀌면 이동 장비는 홈 에이전트에게 알려 재등록

모바일 IP

- 모바일 IP 에이전트 등록
  - 등록 요청과 응답 메시지
    - 전송 계층의 UDP(User Datagram Protocol)에 의해 전달
      - 에이전트는 UDP 434 포트에서 등록 요청
      - 모바일 노드가 사용한 임시 포트로 응답
  - 등록 과정
    - 이동 장비가 사용하는 CoA의 종류에 따른 두 가지 방식
      - 직접 등록(공존 CoA)
        1. 이동 장비가 홈 에이전트에게 등록 요청 메시지 전송
        2. 홈 에이전트는 이동 장비에게 등록 응답 메시지 전송
      - 간접 등록(외부 에이전트 CoA)
        1. 이동 장비가 외부 에이전트에게 등록 요청 메시지 전송
        2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에게 전송
        3. 홈 에이전트는 외부 에이전트에게 등록 응답 메시지 전송
        4. 외부 에이전트가 등록 응답을 받아 처리하고 이동 장비에게 전송

모바일 IP

- 모바일 IP 에이전트 등록
  - 등록 요청 메시지 포맷



모바일 IP

- 모바일 IP 에이전트 등록
  - 등록 응답 메시지 포맷

모바일 IP

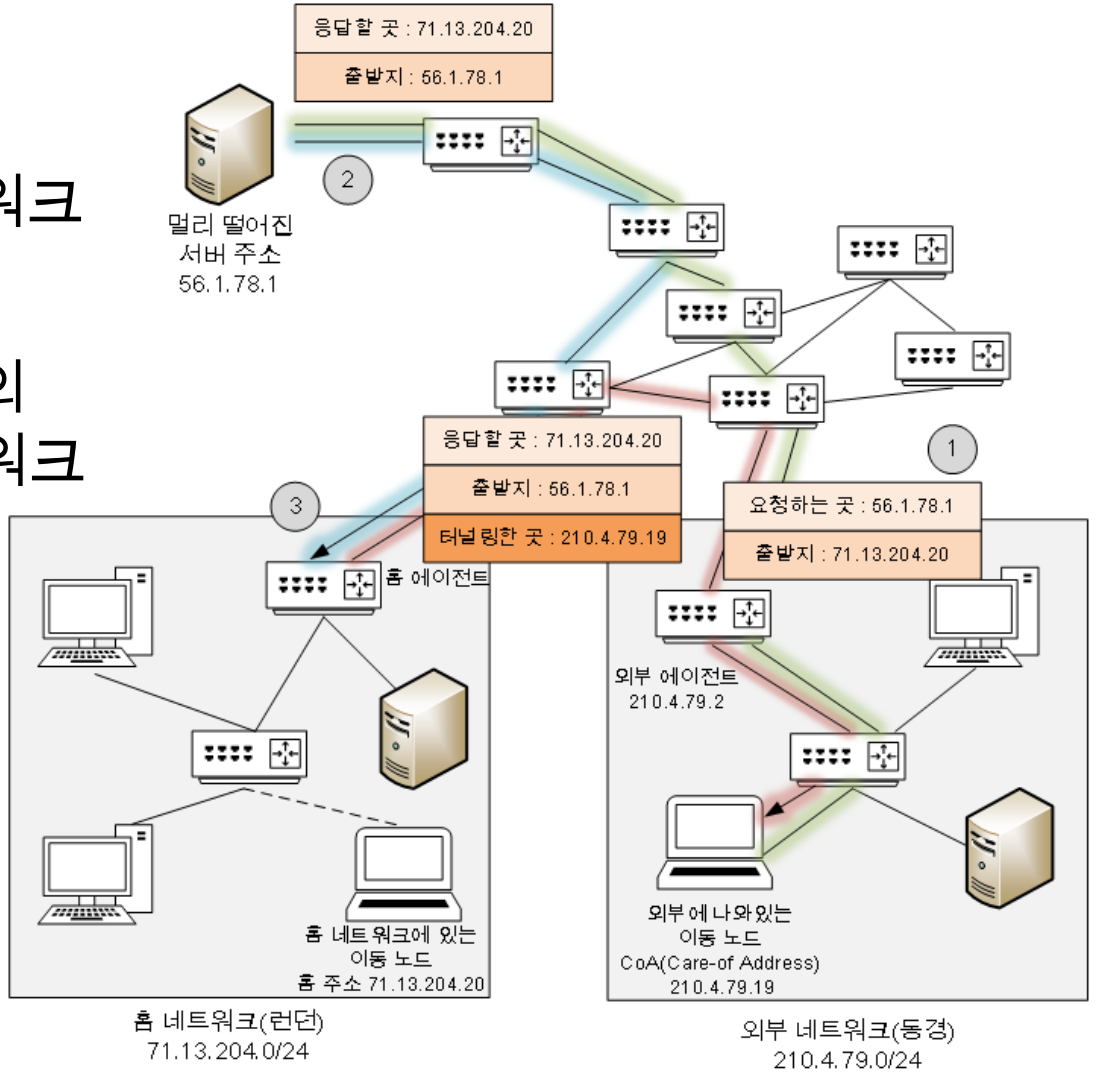
- 모바일 IP 데이터 캡슐화와 터널링
  - 등록을 끝내면 패킷 전달 과정이 활성화 됨
  - 홈 에이전트는 패킷을 캡슐화하여 이동 장비의 CoA로 전달
  - 캡슐화 과정
    - IP 내 IP 캡슐화(IP in IP, IP encapsulation within IP)
      - 한 IP 패킷을 다른 IP 패킷의 페이로드로 만드는 방법
    - 캡슐화하는 장비와 캡슐화를 해제하는 장비 사이에 논리적 터널 생성
      - 터널
        - 홈 에이전트가 이동 장비에게 패킷을 전달할 때에 사용
        - 캡슐화된 패킷의 자세한 정보를 임시로 숨겨두는 역할

모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 모바일 IP 터널링
    - CoA의 종류에 따라 이동 장비와 홈 에이전트 사이, 또는 외부 에이전트와 홈 에이전트 사이에 생성
    - 외부 에이전트 CoA
      - 외부 에이전트에서 터널이 끝남
      - 홈 에이전트에게 받은 캡슐화된 패킷의 IP 헤더를 벗겨내고 원본 패킷을 이동 장비에게 전달
      - 외부 에이전트는 데이터 링크 계층을 통해 패킷을 이동 장비로 전달
    - 공존 CoA
      - 이동 장비에서 터널이 끝나고 이동 장비가 캡슐화 헤더를 벗겨냄

모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 모바일 IP 터널링
    - 동작 과정 그림
      1. 이동 장비는 외부 네트워크에 있는 노드에게 요청
      2. 해당 노드는 이동 장비의 출발지 주소인 홈 네트워크로 응답 메시지 전송
      3. 홈 에이전트는 도착한 응답을 이동 장비에게 터널링

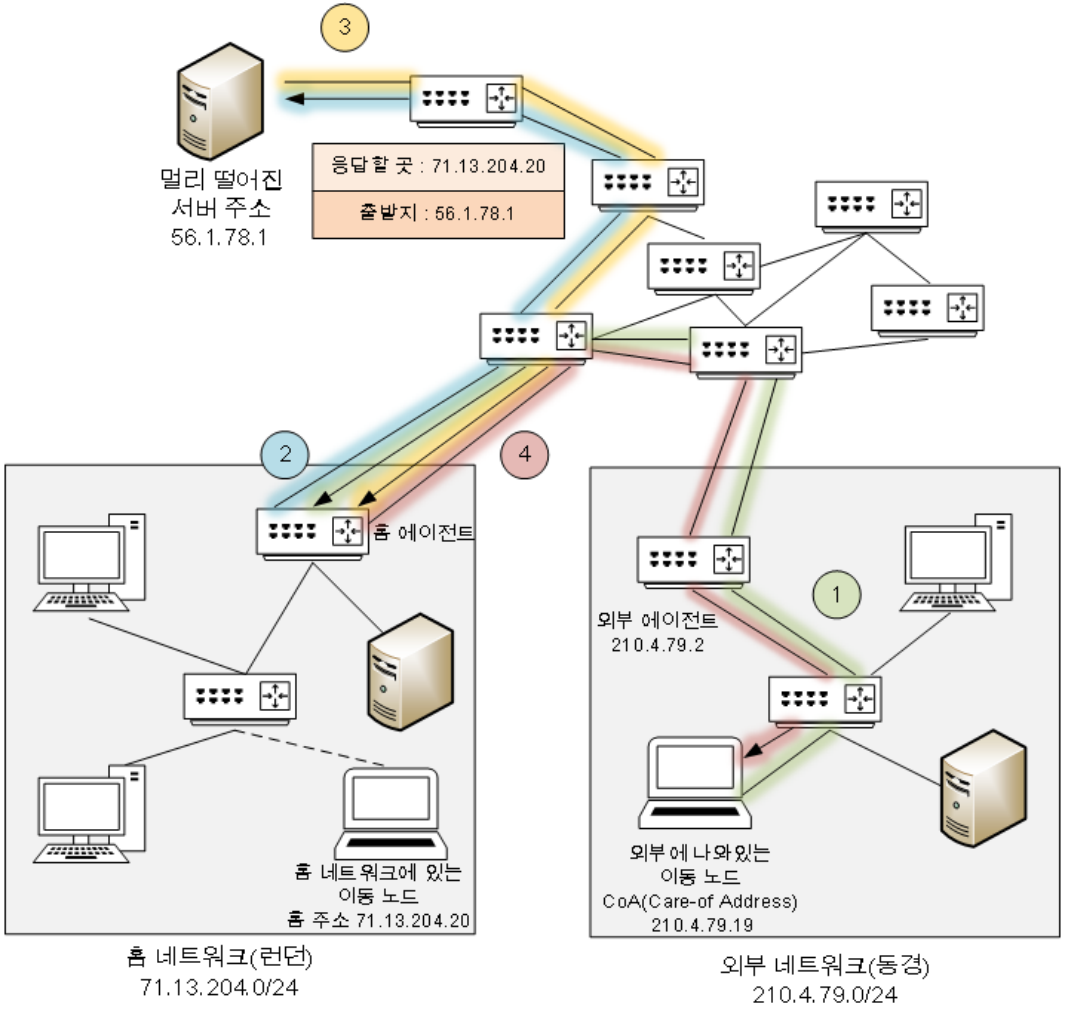


모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 모바일 IP 역터널링
    - 이동 장비와 홈 에이전트에 역터널링이 구현되어 있어야 함
    - 모든 패킷 전송은 홈 에이전트를 통하여 전송
      - 이동 장비는 패킷을 직접 전송하지 않음
    - 총 4번의 전송 과정이 필요하기 때문에 비효율적

모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 모바일 IP 역터널링
    - 동작 과정 그림
      1. 이동 장비가 전송할 패킷을 홈 에이전트에게 전송
      2. 홈 에이전트가 대신 외부 네트워크에 있는 노드로 패킷 전송
      3. 외부 노드는 홈 에이전트로 응답 메시지 전송
      4. 홈 에이전트는 역으로 터널을 구성하여 이동 장비에게 패킷 전달

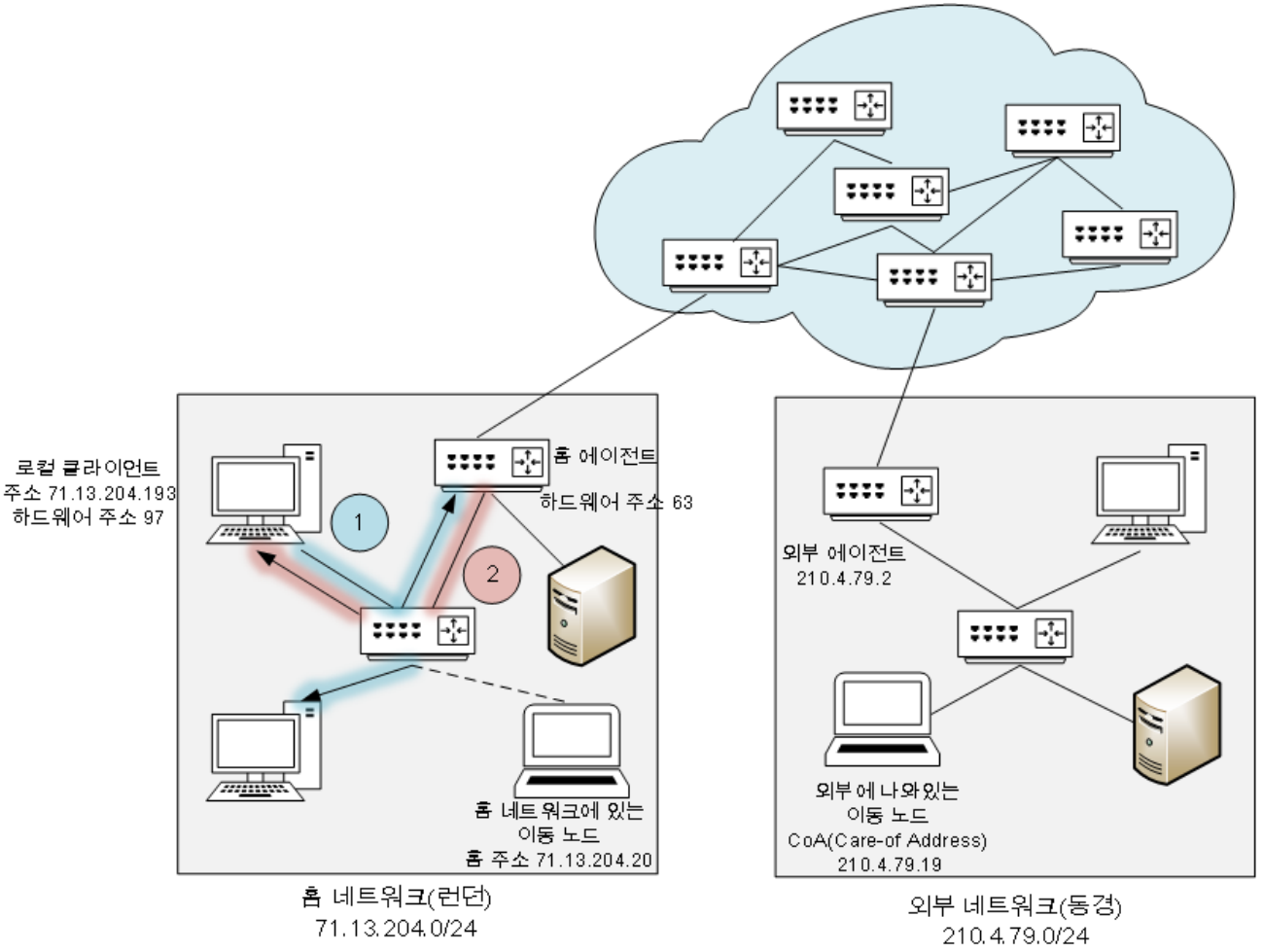


모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
  - ARP를 이용해 홈 네트워크의 다른 호스트가 이동 장비에게 2계층 주소로 패킷을 직접 보내고자 할 경우
  - ARP 문제 해결을 위한 두 가지 작업
    1. ARP 프록싱
       - 홈 에이전트가 로컬 호스트 ARP에 자신의 2계층 주소를 알림
       - 호스트는 이동 장비의 2계층 주소인줄 알고 패킷 전송
       - 홈 에이전트는 받은 패킷을 이동 장비에게 전송
    2. 무상 ARP
       - 홈 에이전트가 이동 장비의 IP 주소에 해당하는 데이터 링크 주소가 홈 에이전트와 같다고 알림
       - 각 로컬 호스트들은 캐시를 갱신

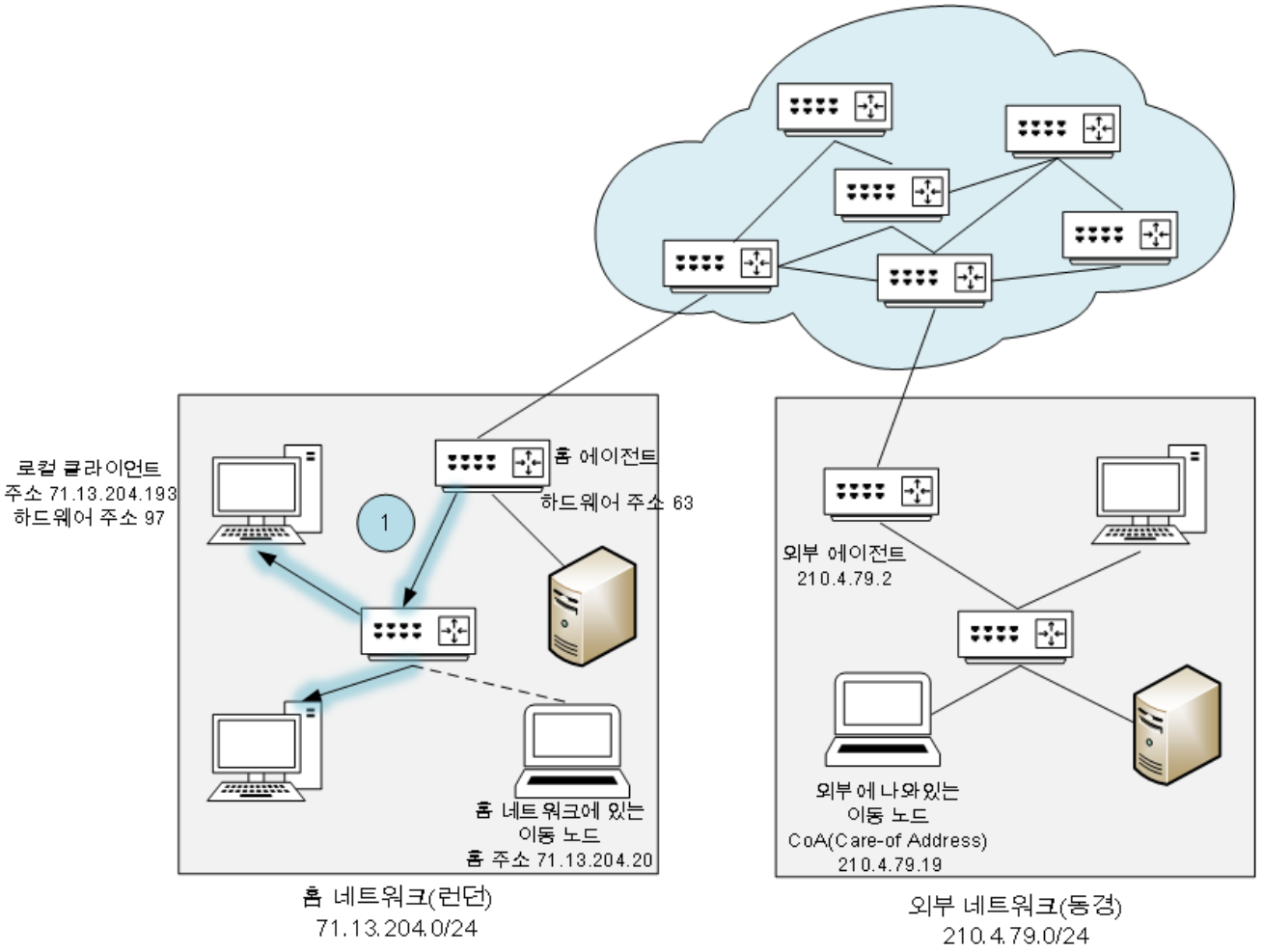
모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
  - ARP 프록싱
    - 동작 과정 그림



모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
  - 무상 ARP
    - 동작 과정 그림



모바일 IP

- 모바일 IP 효율 및 보안 문제
  - 효율
    - 전송자와 이동 장비의 홈 네트워크의 거리에 따라 비효율 정도가 결정
      - 이동 장비와 패킷을 보내는 장비가 같은 로컬 네트워크인 경우 효율성이 떨어짐
  - 보안 문제
    - 주로 무선 통신이 많이 사용하기 때문에 보안에 취약
      - 무선 통신은 본질적으로 유선 통신보다 보안에 취약함
    - 등록 요청과 등록 응답 과정에서 쉽게 공격 가능
      - 모든 모바일 IP 장비에 인증을 지원해야 함
    - 추가적으로 인증과 기밀성을 위해 IPsec의 AH나 ESP를 사용할 수 있음

감사합니다!